

<PROCEEDING> WT Docket No. 06-150, PS Docket No. 06-229, WP Docket No. 07-100
<DATE> 04/11/11
<NAME> Dr. Vijayarangam Subramanian
<ADDRESS1> Idaho National Laboratory
<ADDRESS2> PO.Box 1625, MS 3765
<CITY> Idaho Falls
<STATE> ID
<ZIP> 83415
<LAW-FIRM>
<ATTORNEY>
<FILE-NUMBER>
<DOCUMENT-TYPE> CO
<PHONE-NUMBER> 208-526-0870
<DESCRIPTION> Email Comment
<CONTACT-EMAIL> Rangam@inl.gov

<Text>

Dear Jennifer/ FCC Public Safety Bureau team:

Please find the Idaho National Laboratory comments to the “Third Report and Order and Fourth Further Notice of Proposed Rule Making”. We have specifically focused our comments on the Interoperability Testing (IOT), Section IV.D., of the rule making but we are open to engaging on any other technical aspects as outlined in Section IV, if needed.

All comments have been provided without bias towards any specific provider of the public safety interoperability testing services for the nation.

Warm Regards,
Rangam.

Dr. Vijayarangam Subramanian
Idaho National Laboratory, Idaho Falls, ID 83415
Rangam@inl.gov, 208 526 0870

INL RESPONSE

TO

IV. FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING, FCC-11-6A1-25

D. Testing and Verification to Ensure Interoperability

1. Conformance Testing

106. Interoperability requires that user devices and network equipment comply with relevant standards specifications. Conformance testing, a process generally planned and developed by industry organizations and conducted by certified labs, is a mechanism that could be used to ensure that devices and network equipment that are deployed in the public safety broadband spectrum are compliant with the 3GPP LTE Release 8 and higher standards. We therefore tentatively conclude that we should require that all user devices be subject to conformance testing and seek comment on this tentative conclusion.

[INL Response] With multiple user devices and OEMs that might potentially serve the Public Safety user community, INL supports that interoperability and protocol conformance testing be performed on the user devices and network equipment prior to field deployment and use. RF and protocol conformance testing and integrated security testing should be performed on the user devices by industry organizations and certified labs. This will serve as a preliminary gating process for user devices, before testing at the IOT facility.

108. We also seek comment on conformance testing for LTE infrastructure equipment. Is there any known conformance testing with some formal certification process for LTE infrastructure equipment, namely EPC, including eNodeB, MME, SGW, PGW and PCRF? To what extent is such process used by commercial network providers? Would the benefit of such certification outweigh the possible costs associated with creating a certification requirement for public safety broadband network infrastructure equipment? Finally, we seek comment on who should represent public safety at PTRCB? Should it be the PSST, NIST or another entity? Could it be a combination of entities working in partnership? What is the cost of such a requirement?

[INL Response] Cost optimized protocol conformance certification testing operations are possible when repeated testing over large volumes of similar hardware and software is performed. While the user devices protocol conformance certification testing will support the volume requirement, the core network infrastructure will not.

New infrastructure deployments, hardware revision changes, minor software patches and major software releases, can all contribute to protocol non-conformance of infrastructure in the public safety network and needs to be thoroughly tested before deploying in the field.

Every public wireless network configuration is different. This demands protocol conformance testing under appropriate parametric configurations, hardware configuration, system configuration, policy implementation, QoS requirements, intended applications etc. Hence, a dedicated core infrastructure is needed to perform IOT consistently. In general, the core network hardware and software do not go

through fast evolution with new user equipment hardware and software as the end user devices do. However, hardware and software revisions with bug fixes or enhanced new applications are to be expected, with the base hardware and software platform retained over several years.

Capital requirements to build and maintain separate labs, logistical issues and ROI issues for isolated network infrastructure protocol conformance certification testing can be prohibitive. Hence, it will be beneficial to perform conformance testing (as against performing conformance certification testing) as an integral component of public safety interoperability testing, in addition to the self-certification requirements already practiced by the infrastructure OEMs.

However, if there is an entity that might be available in the future to do customized LTE network infrastructure protocol conformance certification testing for public safety, and approved by other major carriers as well, it should be welcome.

2. Interoperability Testing (IOT)

109. In the Waiver Order, we required waiver recipients to self-certify their performance of IOT on specified LTE interfaces.⁴ We sought comment in the Technical Public Notice on whether our final rules should require only self-certification, or whether we should establish a more formal mechanism for ensuring compliance with any interoperability testing requirements adopted in our final rules. Motorola recommends “self-certification relying on test suites developed specifically for public safety use of Band Class 14.”⁵ Meanwhile, Harris argues that “a self-certification process is adequate in the near term, particularly for systems constructed under the waiver process because final network technical specifications are still being finalized.”⁶ The District of Columbia, however, contends that, “[t]hough self-certification may be sufficient initially, vendors’ desire to differentiate themselves in the marketplace can create incentives that run counter to the goal of interoperability” and “[i]n time, demonstrated interoperability on key interfaces will probably be necessary.”

110. IOT is an important mechanism for ensuring that public safety broadband networks are technically capable of supporting roaming. We therefore tentatively conclude that we should require that public safety broadband networks perform IOT for the LTE roaming interfaces identified in the Third Report and Order above. To this end, we tentatively conclude that we will require that network operators perform IOT, prior to deployment of any RAN equipment, on the following LTE interfaces:⁸

** Uu – LTE air interface*

** S6a – Visited MME to Home HSS*

** S8 – Visited SGW to Home PGW*

** S9 – Visited PCRF to Home PCRF for dynamic policy arbitration*

111. We seek comment on this tentative conclusion. What are the costs and benefits of IOT on roaming interfaces? Have we identified an appropriate list of interfaces on which IOT is necessary to ensure roaming capability among public safety broadband networks? Are there interfaces that should be added to this list, and if so, what would be marginal costs associated with requiring IOT for such interfaces?

[INL Response] IOT on Roaming Interfaces:

One of the primary goals of a public safety network will be to ensure roaming across local, state and regional network boundaries, and across different public safety organizations. Also roaming across the commercial networks and public safety network should also be possible for improving access coverage, reliability backup situations and other possible public safety scenarios.

Based on the eventual technical network architecture that will emerge for the public safety network, different types of infrastructure elements in a LTE network may be sourced from different OEMs. Indeed the same type of elements (e.g. eNodeB's) may be sourced from multiple vendors to encourage competition. Also, the end user devices can be from multiple vendors. Hence interoperability testing on roaming interfaces will be a fundamental requirement.

Network elements keep evolving in hardware and software. This evolution can be expected to be much more rapid than the traditional public safety LMR systems. With LTE technology still in the very preliminary stages of deployment across the world with very little public safety customization, major software releases once every two years, minor software releases once within 3-6 months, and several software patches every 2-4 months can be expected in a public safety network deployment. Hence, IOT is needed, not just before deploying the network first time, but on a sustained basis into the future.

Costs vs. Benefits:

During the initial Public Safety network trial deployment period, interoperability will be a requirement to be delivered with accountability by the OEMs. Beyond the initial deployment and for future deployment, end-to-end Inter Operability Tested hardware, software and devices will be needed. Hence, it is important that public safety interoperability national testing center(s) is (are) established quickly, to avoid potential geometrical progression of risks in deploying non-interoperable networks.

Establishing national interoperability centers could involve significant capital investments (which can run into several tens of millions of dollars, based on the scope of work, number of approved vendors for each element of the network, the network architecture chosen to deploy public safety networks, and maintenance costs). However, the costs of performing integrated wireless-cyber interoperability testing before field deployment of hardware, software and devices, can not only save billions of cumulative dollars across the state, local, tribal and federal agencies but also prevent significant delays in deploying and maintaining reliable, resilient networks. Untested interoperability problems introduced can bring down operational networks leading to major safety and security risks both for the public safety personnel and people in the affected regions. Interoperability testing centers can also help promote standardization and policy formation collaborating with national agencies, as well as provide hands on interoperability training for the thousands of public safety agents across the nation.

Interfaces to Test:

The interfaces already listed in this FNPRM are a great start. However, there can be other interfaces added based on public safety network architecture and features (e.g. addition of IMS core). Also, the interface requirements can differ based on the type of connected network. For example, PS to PS network interoperation can have different security, priority and QoS requirements than PS to Commercial or PS to Federal agencies interworking.

112. Commercial network operators rely on IOT to ensure multi-vendor interoperability for devices and equipment that operate on their networks. The LTE interfaces relevant to multi-vendor interoperability include:

- * S1-u – between eNodeB and SGW*
- * S1-MME – between eNodeB and MME*
- * S5 – between SGW and PGW*
- * S6a – between MME and HSS*
- * S10 – between MMEs*
- * S11 – between MME and SGW*
- * SGi – between PGW and external PDN*
- * X2 – between eNodeB and eNodeB (for intra-network handover)*
- * Gx – between PGW and PCRF (for QoS policy, filter policy and charging rules)*
- * Rx – between PCRF and AF located in a PDN*
- * Gy/Gz – offline/online charging interfaces*

113. Should the commission adopt IOT rules to ensure multi-vendor interoperability on public safety broadband networks? What are the potential costs and benefits of such a requirement? Does the preceding list include all of the interfaces on which IOT should be required to support multi-vendor interoperability or are there other interfaces that should be included?

[INL Response] Yes, the commission should adopt IOT rules to ensure multi-vendor interoperability for public safety broadband networks. The interfaces noted are comprehensive, though interfaces might be added based on the eventual architecture of the network.

As mentioned in the INL comments for section 112 there will be considerable costs in establishing and maintaining public safety interoperability test center(s). These interoperability test centers can help train the public safety agents consistently across different vendor equipments and devices in real field-like environments, form teams supporting the design of networks and applications, help troubleshoot field issues, etc. The IOT national centers can also support the public safety agencies to build a reliable vendor ecosystem and cost effective supply chain environment. Consistent delivery of interoperability testing services for public safety agencies will have the capability to drive and deliver technology innovation rapidly, collaborating with the state, local, tribal and federal agencies.

114. Although IOT is critical to ensuring that public safety broadband networks are interoperable, it is our understanding that no specific guidelines for conducting IOT between such networks have been developed. Accordingly, we tentatively conclude that, for the interim, each public safety broadband network operator will be required to submit for Bureau review, within six months of its date of service availability,⁹ a plan for IOT.¹⁰ The scope of the IOT called for in the network operator's plan would be

required to be sufficiently broad to address all LTE capabilities and functions required under the Waiver Order, and it should examine all the interfaces needed for roaming to and from other public safety networks. After the Bureau approves its plan, each network provider will be required to certify, within three months, that IOT will be conducted on an ongoing basis with other deployed public safety broadband networks until final IOT testing rules are adopted.

115. We observe that commercial broadband service providers, who perform IOT to ensure interoperability among devices and network infrastructure, generally own or operate laboratories in which they can perform IOT. Because it is similarly important for public safety networks operators to have access to IOT for the purpose of verifying interoperability, we tentatively conclude that certain lab facilities need to be designated for the purpose of IOT. We seek comment on this tentative conclusion. Are there facilities already available for conducting IOT for public safety broadband networks? Are there third party commercial laboratories where public safety broadband network IOT could take place? How about federal lab facilities such as NIST/NTIA (PSCR) facilities, or the Idaho National Laboratory (INL)? How about an arrangement with certain commercial service providers to conduct IOT for public safety in their own lab? How should the lab facility be compensated? Who should pay for the services? Who should set and manage the set of guidelines for IOT? Who should determine the test plans? Is there a role for the PSST in this process? We note that PSCR is developing test plans for its public safety demonstration network.¹¹ Is it appropriate to use such test plans for IOT? If not, what is an appropriate process for developing test plans for public safety purposes? We seek comment on all of these matters.

[INL Response]

IOT Laboratory:

We support the creation of interoperability lab facility(ies) for public safety IOT. IOT is a complex process for a LTE network due to many different network elements, devices, interfaces, multiple public safety technology interworking scenarios (like legacy LMR/ GSM/ CDMA networks, optical, microwave, satellite backbones), applications, vendors, etc. Hence, as for any major telecom carrier, it is critical to have an IOT laboratory that can serve the nation-wide public safety community. It is common to have parallel close-to-field testbed networks to test different core and RAN elements of the network with various versions of software and hardware that mimic the actual deployed versions against proposed upgrades and software patches. In addition, new applications and devices will be expected to become available on a continuous basis. Hence, consistent, reliable IOT services dedicated for public safety networks will be needed.

3rd Party, National Laboratories for IOT Testing?

It is important to note that there are already 3rd party organizations that perform protocol testing for handsets. There are new efforts by 3rd parties to provide protocol conformance certification testing for the LTE core elements. Today most of the carriers perform protocol conformance testing for core elements in addition to the IOT prior to field deployments. But protocol testing is just one aspect of testing the core elements. Besides the low volume of turnover for the individual core elements and relatively few major and minor software, hardware upgrades every year (discussed in the INL response to sections 108 and 111) make it challenging for 3rd party dependence on protocol conformance certification for core elements.

However, as queried in the comments by the commission in section 115, we are not aware of any private or national agency yet designated to perform public safety LTE IOT. Protocol testing of lower layers for each individual element is just one aspect of testing and does form a pre-cursor to a customized public safety interoperability testing. If no viable LTE core network element protocol conformance certification testing entity is identified, the public safety IOT test center could perform protocol compliance verification for the core elements as an integral component of performing IOT.

Depending upon the evolution of the public safety network architecture, two major scenarios can emerge which will determine the operational complexity of the IOT test center(s).

Scenario 1 – Public Safety Network of Networks: Different agencies can build separate networks with exclusive, physical control of the networks, but with a common backbone using 3rd party providers. Also, common cost efficiency elements at the core of the network are possible, for home location registers, authentication, billing support etc.

Scenario 2 – One common public safety network can cover all agencies in the nation: Different agencies can have soft(ware) control of their territory, with one operator building and maintaining the network.

From the perspective of interoperability and building a long-term program for IOT testing, Scenario-1 will provide the toughest challenge, with multiple network operators. Scenario-2 will be served better, having a single operator. Based on how the operations are structured, there can be different entities other than the operator to support development of new technologies and applications for public safety use, as well as performing secure, unbiased interoperability testing before the operator deploys the hardware and software in the field. This national facility(ies) can become the national training center for secure wireless networking for the public safety agencies, besides supporting national rule making and policy formation.

We note that the PSCR, NIST/NTIA facility in Boulder, CO is leading the LTE demonstration efforts for public safety agencies besides developing the PS LTE test plans and supporting the development of overall architecture for the public safety network. We believe that this facility is well positioned in supporting all the front end activities for performing the IOT, including support for policy and rule making, network architecture, feature planning, test plans development, coordination for developing networking standards etc. Additionally, a national IOT laboratory(ies) with appropriate assets and capabilities for performing unbiased cyber integrated IOT, assisting with operator network design and deployment, training public safety agents and providing network field support etc., can be very complimentary to the activities of PSCR and the actual network operators, who will be building and operating the network.

The national assets and capabilities available at the Idaho National Laboratory is an example of a facility that can appropriately complement and support the national public safety broadband communications interoperability testing needs. The INL has a unique 890 square mile test range, located in southeastern Idaho, approximately forty-five (45) miles west of Idaho Falls, ID, providing controlled, quiet, radio frequency (RF) spectrum with minimal background interference from rural/urban areas, airports or military test ranges. The INL has expertise using an extensive set of isolated, commercial-grade, Tier-1 test networks, including, GSM, UMTS, CDMA, WiFi, WiMAX (mobile & fixed), HF/VHF/UHF, WiFi, SONET, LMR, and Satellite communications systems, in addition to limited UAV test facilities. There is also a highly trained technical pool with expertise in wireless, cyber security and control systems

technology research, development, testing, integration, development, deployment, technology transfer and training.